Improving the redistribution of the security lessons in healthcare: An evaluation of the Generic Security Template

Ying He* [1] , Chris Johnson [2]

[1] *School of Computer Science and Informatics, De Montfort University, UK*
[2] *School of Computing Science, University of Glasgow, UK*

Abstract

Context. The recurrence of past security breaches in healthcare showed that lessons had not been effectively learned across different healthcare organisations. Recent studies have identified the need to improve learning from incidents and to share security knowledge to prevent future attacks. Generic Security Templates (GSTs) have been proposed to facilitate this knowledge transfer. The objective of this paper is to evaluate whether potential users in healthcare organisations can exploit the GST technique to share lessons learned from security incidents.

Methodology. We conducted a series of case studies to evaluate GSTs. In particular, we used a GST for a security incident in the US Veterans' Affairs Administration to explore whether security lessons could be applied in a very different Chinese healthcare organisation.

Results. The results showed that Chinese security professional accepted the use of GSTs and that cyber security lessons could be transferred to a Chinese healthcare organisation using this approach. The users also identified the weaknesses and strengths of GSTs, providing suggestions for future improvements.

Conclusion. Generic Security Templates can be used to redistribute lessons learned from security incidents. Sharing cyber security lessons helps organisations consider their own practices and assess whether applicable security standards address concerns raised in previous breaches in other countries. The experience gained from this study provides the basis for future work in conducting similar studies in other healthcare organisations.

Keywords: Generic Security Template, lessons learned, security incident, knowledge

redistribution, healthcare.

1. Introduction

Security incidents have affected healthcare organisations across the world. For example there are strong similarities between the US Veterans' Affairs Administration (VA) 2007 data loss incident [1], the Shenzhen 2008, the Chinese data loss incident [2] and the UK National Health Service (NHS) Surrey security Asset disposal incident [3]. However, these examples are just the tip of the iceberg. Symantec reported that the healthcare industry accounted for 36% of all security incident breaches in 2013 [4]. At 44%, the healthcare industry continues to be the sector responsible for the largest percentage of disclosed data breaches by industries in 2014 [5]. Such incidents can result in the loss of company/organisational reputation and customer confidence, legal issues, a loss of productivity and direct financial losses [6]. The focus in Healthcare lessons learned and information exchange has been on safety [7–13] rather than security [14–16].

Governments have realised the importance of learning from security incidents. A number of initiatives support the exchange of information about previous breaches. For example, the UK government has launched the Cyber Security Information Sharing Partnership (CISP). This is intended to help government and industry share and redistribute intelligence on cyber security threats. The partnership includes the introduction of a secure virtual 'collaboration environment' where stakeholders can exchange information on threats and vulnerabilities in real time [17]. There is a need to foster an environment where different parties can speak the same language while redistributing this information.

The recommendations and insights derived from previous security incidents are usually disseminated through a series of formal and informal reports, meetings and presentations to management [18, 19]. For example, NHS disseminates lessons learned from security incidents using team meetings, notice boards, incident reporting and investigation training courses (e.g. use of case studies), email, newsletter, internal alert systems and so on [20]. Meetings are held and notes are gathered to document responses, disagreements, suggestions and additions to security policies

*Corresponding author: ying.he@dmu.ac.uk (Ying He)

and incident procedures [18]. Issues to document include the effects of the damage, actions taken during the incident, policies and procedures that require a change and evidence that can be used for pursuing the responsible person(s) [21]. It is expected that healthcare organisations will act on these lessons, for instance by changes in procedures or training processes and incident response policies. However, previous case studies show that security lessons have not been effectively re-distributed within many organisations [22–24].

Generic Security Templates [25] have been developed to represent lessons learned from security incidents. They extend the application of the existing Goal Structuring Notation (GSN) [26] to support the exchange of lessons learned in the aftermath of data breaches. GSTs represent the links between particular findings and the requirements of security standards and policies at a level of abstraction that is intended to support reuse. In this paper, we conducted a series of studies to evaluate whether users can exploit GSTs to redistribute lessons learned from a specific security incident from the US Veterans Affairs Administration into a healthcare organisation in China.

The remainder of the paper is structured as the following. Section 2 reviews related work. Section 3 introduces GSTs. Section 4 presents our first evaluation of this approach, GST acceptance testing. Section 5 presents a second evaluation, the implementation of the approach within a Chinese healthcare organisation. Section 6 discusses the findings, and Section 7 summarises conclusions and future work.

2. Related work

2.1. Incident learning

A key activity in Security Incident Response and Handling (SIRH) is to learn from errors or mistakes made during previous incidents. It is important to identify policies and processes that undermine existing defences. It is also important to identify any weaknesses in staff competency. These insights must then be fed-back into security management processes [18, 19]. Recent studies have provided rich controls for preventing information security threats and vulnerabilities, including technical countermeasures (e.g., anti-virus software tools), and organisational defences (e.g. security standards). However, reflection on security incident response is typically limited to the

technical process and does not leverage opportunities to learn about the security threat environment and the effectiveness of internal procedures, controls, training and policies in order to strengthen the organisation's information security management systems [27, 28]. There is relatively little research into effective means of disseminating security recommendations and best practices between organisations. The lessons from previous security incidents contain rich information about the causes of previous breaches. Failure to learn from previous incidents seems to be a common trait across many different kinds of security incidents [23].

2.2. Incident learning in healthcare

The loss of patient data can affect both the individuals concerned and healthcare organisations responsible for securing that data. If a patient's information is disclosed accidentally or unintentionally, it may constitute an infringement of privacy. Disclosure can cause embarrassment. It may also have an impact on an individual's career. The loss of patient data can have other long-term financial implications, including the loss of health insurance [29]. Data can also be sold on to other criminals, for example to support identity theft. From the perspective of healthcare organisations, security incidents can cause significant damage to reputation. They may also lead to fines, for instance under the new European Commissioners' Data Privacy Directive (Directive 95/46/EC) [30]. Therefore it is imperative for healthcare organisations to learn the lessons that have been identified following previous incidents and take actions to prevent any recurrence.

In Europe and North America, there are legislative requirements to report security incidents [20, 31, 32]. A key aim of incident reporting is to prevent any future recurrence of previous incidents not only in the organisation where the incident occurred but in other healthcare institutions [20]. In China, there have not been legislative requirements for healthcare organisations to report or exchange security incidents. Partly in consequence, information security has not attracted significant attention from healthcare providers [33, 34], although some attempts have been made to protect patient data [35–38]. Gao suggests two main reasons for the lack of motivation: (1) the Chinese traditional culture does not address the importance of personal privacy; and (2) healthcare systems in China are still in their infancy and there has not been large-scale health data exchange that can potentially trigger large amounts of privacy violations [39]. However, the implementation

of healthcare information systems can hardly be successful if information privacy cannot be ensured [40]. There is a need to learn successful practices from international experience to improve healthcare security management systems [39].

3. Generic Security Templates (GST)

This section introduces GSTs and related work. GSTs build on previous research into safety assurance cases [41]. Instead of collecting evidence to argue that the design and operation of an existing application is acceptably safe, GSTs collect the insights that have been derived when a system has proven NOT to be acceptably secure. They represent security lessons (i.e. information about the causes of a breach and subsequent recommendations) from previous incidents and map them to the requirements of healthcare information security management systems.

3.1. Definition of the Generic Security Template

A *Generic Security Template* is "a documented body of lessons identified from a security incident that is intended to provide feedback about the implementation of specific security standards or guidelines " [25]. The GST links the analysis of an incident to specific security standards or guidelines that help to implement particular recommendations. Figure 1 provides a customised Goal Structuring Notation from the domain of safety analysis for our cyber security GSTs. There are four principal syntactic components, A *Goal* is a claim, the statements that the goal structure is designed to support. *Lessons learned* exist to support different levels of goals. It refers to the security issues (causes of a security incident); and the security recommendations that are intended to avoid any recurrence of a data breach [25]. *Strategy* is inserted between goals at two levels of abstraction, to explain how the top-level goal is addressed by the aggregation of sub-goals. *Context* is used to declare supplementary information and provide adequate understanding of the context surrounding the claim/strategy. Usually it presents concepts clarification introduced in the claim/strategy [42]. Examples of the application of GSTs can be found in [25, 43–45].

3.2. Represent security lessons using the GST

GSTs provide a graphical overview of the mapping between the causes/recommendations derived from security incidents and the guidelines/policies/standards/regulations that are intended

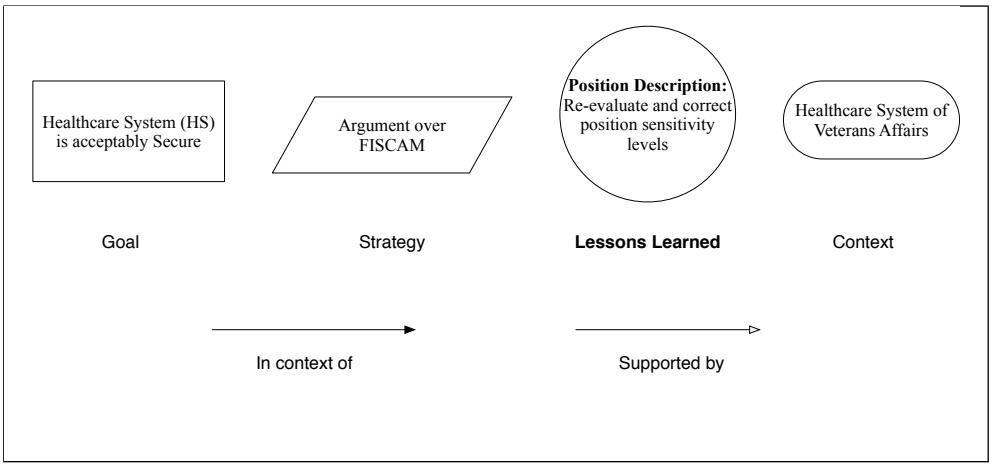

Figure 1: Customised GSN Notations for GST

to prevent any recurrence of a data breach. The following section summarises the steps that are needed when a GST is developed to represent a security incident. Figure 2 provides an example instance created for a real world case study, the US Veterans Affairs' Administration data loss incident from 2007 [1]. More details can be found in [25, 43].

- *Prepare the Goal Structure*. The top level goal is to ensure that a healthcare system is acceptably secure in the aftermath of an incident. This high-level goal is then decomposed into sub-goals that each reflects more detailed objectives within a security management system. The GST identifies sub-goals by using security requirements within the applicable standards and guidelines in particular healthcare organisations. For example, the example in Figure 2 used the structured category of security requirements of the General Control in Federal Information Security Control Audit Manual (FISCAM) [46] as the goal structure.

- *Identify the Lessons Learned from the security incident.* Lessons learned are identified by searching incident reports for security recommendations. These are then introduced into the GST using a structured textual format. For each security issue, the GST uses short <Noun-Phrase> sentences, for example, "Sensitive Information", to describe specific security issue. For the recommendation, the GST uses <Verb-Phrase> <Noun-Phrase>, for example, "Use encryption or effective tool to protect personal identifiable information" to describe security

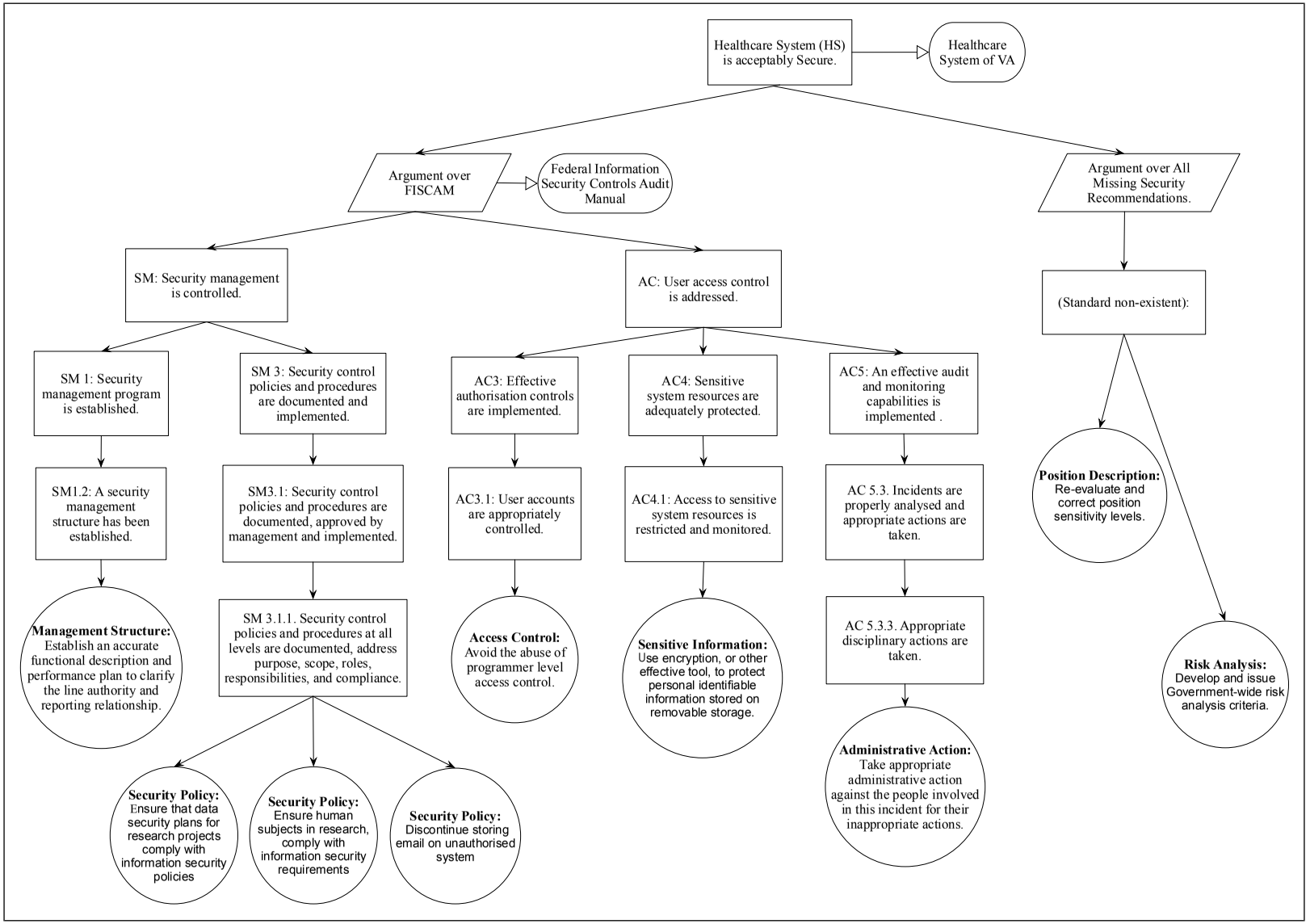

Figure 2: The GST created for the VA Dataloss Incident

recommendations.

- *Map Lessons Learned to the Goal Structure.* The lessons learned are then mapped to different levels of the goal structure. The analyst has to identify the relationships between security sub-goals, based on standards, guidelines and policies, and the lessons learned from a previous security incident. Figure 2 shows how lessons can be introduced into a GST at different levels of abstraction.

- *Elaborate the Context and Strategy*. Strategies are inserted between goals and sub-goals. They justify goal decomposition. Thses typically refer to the security standards, organisational guidelines, regulations and policies. The GST exploits a simplified sentence structure, for example, "Argument over FISCAM" to describe strategies. Context was used to provide supplementary information for a specific incident. The context notations are elaborated during this process. For example, "Federal Information Security Controls Audit Manual", is used to explain the concept "FISCAM" in the strategy.

4. Evaluation 1 - acceptance of the GST

4.1. Target Organisation

A five months internship was accepted in 2013, with a Chinese healthcare organisation, the redacted hospital. The internship was to support a newly initiated Security Strengthening Program (SSP). The redacted hospital started using an electronic healthcare system from 2008 and was looking for recommendations to improve their security system. This internship provided an opportunity to obtain more knowledge about information security management in healthcare organisations in China and their support enabled us to conduct an exploratory case study.

The host organisation is a tertiary level hospital in China and has the highest level of maturity in terms of healthcare information systems. Its security management is subject to compliance regulation through security standard GB/T22239 (Information security technology - Baseline for classified protection of information system) [47]. This Chinese security guidance uses a five-level classification system. Organisations are required to comply with the GB/T22239, by achieving an appropriate level. For example, the guidance of the health industry information security level

protection issued by the Ministry of Health of the Peoples Republic of China requires that health information systems and related units should be self-examined in accordance with GB/T22239. In particular, the tertiary level hospital needs to achieve at least the third security level characterised in GB/T22239 [48].

4.2. Participants

To understand different stakeholders' acceptance of GSTs, we interviewed people from different roles which included healthcare professionals (doctors, nurses) and security professionals. Since the aim of the study was to explore users' experiences of the GST approach, rather than generalising the results, we focused on a small number of participants. This provided suitable coverage of stakeholders across the organisation. Information sheets were disseminated to each department of the redacted hospital and details were put up on notice boards. The participants attended the study voluntarily. The study adhered to the BPS ethical guidelines, and had been approved by an ethics committee of the University of Glasgow (ref: CSE01243). Participants completed a consent form before starting the study.

4.3. Study design

This evaluation was intended to identify general attitudes towards the use of graphical structures to represent lessons learned in previous security breaches. The participants were presented with the specific security diagram created for the VAs 2007 data loss incident, illustrated in Figure 2. They were given a tutorial that introduced the notations and approach. They were given some time to study the graph and were then asked questions. The interview started after the participants had clarified any remaining concerns about the approach. This interview compared the GST with any existing methods used to redistribute lessons from security incidents.

Due to the explorative nature of this study, we conducted unstructured interviews during normal working hours. We were not allowed to record the conversation due to the sensitivity of the research themes. In qualitative data analysis, transcription, analysis and verification are interwoven before, during and after data collection [49]. This iterative approach was utilised in the current study and reflects the constraints on any research of this nature across national borders in critical

environments. For example, during data collection and transcription, possible ideas and questions were noted down. After the interview, a summary based on the transcribed interviews was sent to participants, for validation. The field notes were then coded and these codes were categorised in relation to technology acceptance frames [50]. The data was further cross-referenced with the collected document for triangulation [51].

4.4. Results

4.5. Participants background

The healthcare professionals who participated in this study, included four doctors (males) and six nurses (females). Five security professionals participated in this study, four of them were security engineers (one female and three males) and one of them was a security manager (male). The educational background of the security professionals ranged from those with a BSc qualification to those with the equivalent of an MSc. All of the security engineers had experience with security incident handling. Among the healthcare professionals, two nurses and one doctor had been involved in the security incident handling process. The rest had no experience with information security. Further background information is summarised in Appendix A.

4.6. Attitudes towards the GST

The participants were presented with a GST instance as shown in Figure 2. They were then invited to comment on the GST. The security professionals and healthcare professionals demonstrated different perspectives towards the use of the GST. According to Orlikowski and Gash [50], various organisational stakeholders interpret technology in different ways. An understanding of people's interpretations of technology is critical to understanding their acceptance of it [50]. We adopt Orlikowski and Gash's idea of technological frames to analyse our results.

- *Nature of Technology*, refers to people's perceptions of the technology and their understanding of its capabilities and functionalities.
- *Technology Strategy*, refers to people's views of why their organisation acquired and implemented the technology. It includes their understanding of the motivation or vision behind the adoption decision, and its likely value to the organisation.

- *Technology-in-Use*, refers to people's understanding of how the technology will be used on a day-to-day basis, and the likely or actual conditions and consequences associated with such use.

4.6.1. Healthcare professionals' attitudes

Nature of Technology

The healthcare professionals demonstrated a basic understanding of the GST. They considered it to be "some way similar to the communication of security incidents in departmental meetings". They identified the benefits of the GST in representing security incidents. A healthcare professional said, "it makes things clearer, it breaks down issues into details", "we can easily focus on a specific issue they (security professionals) talk about ".

Technology Strategy

The healthcare professionals believed that the use of the GST helped to formalise communication about security incidents, as compared to previous appoaches that relied on informal presentations and meetings. As stated by one of the healthcare professionals, "previously, different security professionals present security incidents using their own language and ideas, but I like this structured way, that makes everything easier to follow". However, there were also concerns raised about using GSTs. As stated by a healthcare professional, "I am not sure if it is necessary to make the changes, as we rarely communicate incidents unless after a severe security incident ".

Technology-in-Use

The Chinese healthcare professionals had some difficulties in understanding technical terms in our GST from the United States VA case study. One participant felt that, "if you had not explained the concept of 'access control', I could not understand it by myself". They suggested either a supporting document providing definitions for technical terms or that they needed help from security professionals. They also complained about the "lack of multi-view design" in the GST. As stated by a healthcare professional, "'access control' seems to be the security professionals' responsibility ". In other words, they would have liked a simplified GST that focusses only on security

lessons for Healthcare professionals and another more detailed diagram for IT security staff.

4.6.2. Security professionals' attitudes

Nature of Technology

Security professionals also found the GST to be effective in representing security incidents. One participant stated that, "this will be especially helpful to discuss security issues; it is easier to navigate between different notations". The security manager stated "it brings together everything that involves different stakeholders; it can facilitate decision making and balance the interests of different stakeholders in a discussion ".

Compared to healthcare professionals, security staff demonstrated a deeper understanding of our GST in terms of its capabilities and limitations. They believed that it was a good way to inform the implementation of security standards. A security professional stated "it provides a process to track what goes wrong at which level in the security standards that causes the incident ". "It can let us know how well we have implemented the security standards and which part needs to be improved". Moreover, they found the lessons which cannot be mapped to any security requirements especially helpful. One security professional said, "this will help us identify a new security requirement that was not considered by the standard".

Technology Strategy

The security professionals believed that, the use of GSTs tended to change the way to report and communicate security incidents. They mentioned that, presenting lessons in this way "helps to identify management causes, which might be the inappropriate implementation of a standard, rather than the specific technical causes". This is consistent with previous studies that organisational security incident handling focusses on direct causes rather than underlying procedures or policies [52]. The security professionals also identified the GST's role as "bringing together information and notes generated in the security incident handling process, and an easier way to track previous lessons".

Technology-in-Use

To use GSTs, security professionals would have to learn a new technique to report security incidents. One of the participants complained "I cannot predict how effective it will be, and how worthwhile the efforts are ". However, from a long term perspective, the security professionals tended to agree that "the benefits might outweigh the efforts once everyone starts getting used to this new technique ". This is consistent with the findings in safety, where GSN has been widely adopted. The proponents of GSN argue that its expressive power repay the cost in learning to use the approach [53].

Participants were also concerned about the scalability of GSTs in everyday use, "the template could become unmanageable for a complex incident or for the integration of many less serious breaches". This issue can be addressed by experience from GSN to improve safety. Our notation also benefits from the modular concepts that have already been used in this existing approach [54, 54]. However, further work is required to apply these techniques to security incidents.

Security and healthcare professionals had different interpretations of the GST. They made the judgments based on their own knowledge, experience and work style. To the healthcare professionals, the GST served as an effective tool to represent security incidents, however, they did not see this tool as essential for their organisation in their everyday work. They were concerned about the effort to learn and adopt such a new technique. In comparison, security professionals identified the advantages in using GSTs to inform the implementation of security standards. Although they might have to learn a new technique, they still believed the long term benefits were worthwhile.

4.6.3. Strengths and weaknesses

Based on the analysis above, the strengths and weaknesses of our approach are summarised in Table 1 and 2.

4.6.4. Scenarios for applying GSTs

The healthcare and security professionals who supported the use of GSTs helped to identify potential scenarios:

Scenario I: communicate security incidents in department meeting. Healthcare professionals found GSTs useful in representing lessons learned from security incidents, and suggested adopting this method for demonstrating security incidents in department meetings in the future.

Table 1: The strengths of the GST

The Strengths	Healthcare Professionals	Security Professionals
Effective Communication	... some way similar to the communication of security incidents in the department meeting ... easier to navigate between different notations ... it makes things clearer, breakdown issue into details ... we can easily focus on a specific issue they (security professionals) talk about ...	... this will be especially helpful to discuss security issues ... easier to navigate between different notations ... it brings together everything that involves different stakeholders ... it can facilitate the decision making and balance the interests of different stakeholders in a discussion ...
Formalised Representation	... previously, different security professionals present security incidents using different ways of their own, but I like this structured way, that makes everything easy to follow ...	... bringing together pieces of notes generated in the security incident handling process, and an easier way to track previous lessons ...
Linkage to Security Management Procedures		... a process to track what goes wrong at which level in the security standards that causes the incident; ... let us know how well we have implemented the security standards and which part needs to be improved; ... this will help us identify a new security requirement that was not considered by the standard or organisation.

Table 2: The weaknesses of the GST

The Weaknesses	Healthcare Professionals	Security Professionals
Learning Efforts	... I am not sure if it is necessary to make the changes, as we rarely communicate incidents unless after a severe security incident ...	... cannot predict how effective it will be, and how worthwhile the efforts are.
Scalability		... template could become unmanageable if it documents a complex incident or it is an integration of many tiny incidents.
Comprehension	... if you don't explain the concept 'access control', I could not understand it by myself ...	
Multi-view Design	... lack of multi-view design ... 'access control' seems to be security professional's responsibility.	

Scenario II: inform the implementation of security standards. Security professionals found GSTs useful in informing the implementation of security standards. Future work is needed to focus on how GSTs can inform the implementation of standards.

A previous study had already provided evidence that GSTs can improve the communication of security lessons compared to traditional text based approaches [45]. The next section, therefore, expands on Scenario II to find out how the GST can be used to redistribute security lessons into security management procedures.

5. Evaluation 2 - redistribution of the security lessons

The interviews with healthcare professionals in China provided initial insights into the application of GSTs. However, we were also anxious to look beyond subjective impressions to provide more direct evidence about whether or not security lessons from previous incidents can be redis-

tributed to the redacted hospital. In particular, we used the diagram for the VA 2007 data loss incident as shown in Figure 2 to investigate whether Chinese healthcare professionals could reuse security lessons from this US incident.

5.1. Study design

In the redacted hospital, whenever a decision in information security has to be made, different stakeholders in the organisation are gathered together to discuss the issues. However, the final decision will be made by the security manager based on these different views. We, therefore, conducted a group study with the participants to gather a range of views about the utility the GST. The relevant security manager within the hospital agreed to participate in the session. Our group consisted of six people working in the redacted hospital. These included three healthcare professionals, two security experts and one security manager.

The interaction among group participants often reduces the need for the moderator to intervene or bias individual members of the group. In this way, group dynamics help to reduce the researchers' influence on the interview process [55]. Group study can stimulate thinking and verbal contributions. In the study, group participants were asked to identify lessons that they could apply from the VA incident. To avoid fatigue the meeting was divided into two sessions. Each one lasted for 1 to 1.5 hours. In both sessions, a security engineer accompanied the researcher and together they maintained field notes to document the group discussion. A set of group study guidelines (open-ended questions) was developed for the moderator including probes designed to refocus the discussion if necessary.

- Does your organisation have security concerns (e.g. "issues with Sensitive Information") issue?
- Do you think these recommendations are helpful for your organisation?
- Would you be able to apply this recommendation?
- What are the barriers for you to apply this recommendation?

5.2. Execution of the first session and results

As mentioned, the security management system of the redacted hospital is based on the Chinese security standard, GB/T 22239. The focus group, therefore, decided to replace the goal structure of the VA 2007 data loss incident, which identified recommendations associated with the implementation of US FISCAM requirements with the equivalent Chinese regulations. They chose to focus on the provisions within GB/T22239 that might help to avoid any similar incident in their hospital. This process lasted over an hour and included a detailed analysis of the clauses in GB/T22239 as well as the VA 2007 incident.

The overall process of replacing the US FISCAM requirements with the provisions of China's GB/T22239 followed the same processes that guided the creation of the incident map. The first two steps "(1) Prepare the goal structure" and "(2) Identify the Lessons Learned from the security incident" were very easy because the goal structure (i.e. GB/T22239) and lessons learned (i.e. leaf nodes lessons learned in Figure 2 were readily available. By following the step "(3) Map the Lessons Learned to the Goal Structure", they decided the mapping of the lessons learned to different levels of the security requirements of the security standard (i.e. GB/T22239). By following "(4) Elaborate the Context and Strategies", they have set the Strategy as "Argument over GB/T22239" and the Context as "The redacted hospital". Figure 3 shows the resulting instance of the GST.

The process of mapping between the US case study and the context in Chinese healthcare yielded some significant insights. For instance, "Risk Analysis" was changed under the stratogy "Argument over All missing Recommendations". It identified a new security requirement that was probably missed by GB/T22239. Several other lessons in the VA case study associated with policy issues, were changed to lessons about "Management Structure" and about the handling of "Sensitive Information". In other words, the Chinese focus group looked more at the implementation and operation of security management systems rather than on the provision of policy documents and guidelines. These differences in emphasis may be due to the particular biases of the Chinese participants. Equally they may also suggest valuable alternative insights that could be communicated back to the VA. The key issue is that the process of applying lessons from breaches in one country to another reveals valuable questions for further research. There seem to be considerable

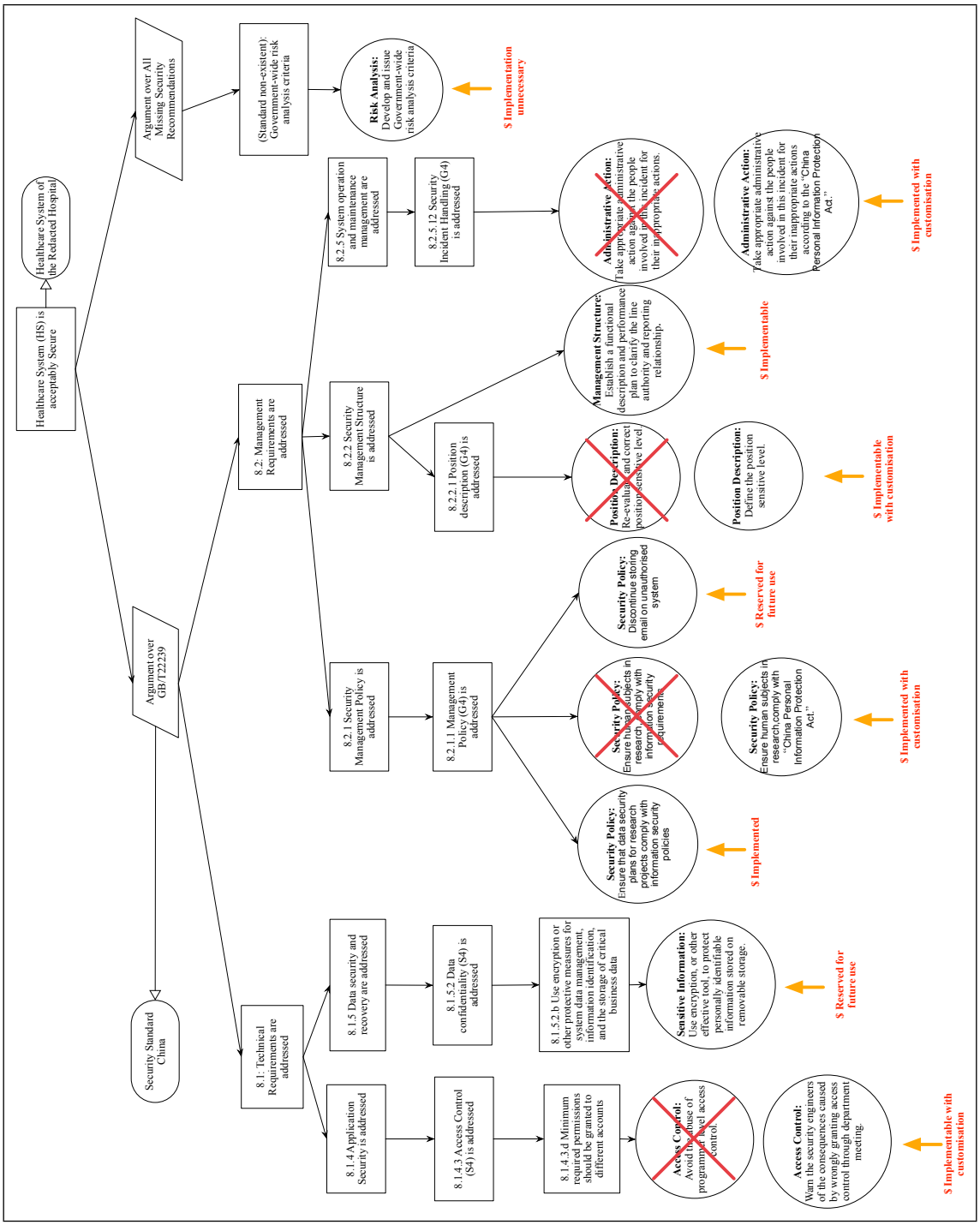

Figure 3: The customised GST for the VA 2007 Dataloss Incident

opportunities to work together to increase the security of patient data in an area that is traditionally characterised by mutual suspicion.

5.3. Execution of the second session and results

In the first session, the focus group related the findings from the VA case study to the provisions in the Chinese standard GB/T22239. They were not asked to consider whether or not they could be implemented within their own healthcare organisation. In contrast, the second session traversed the new diagram to identify any barriers to the application of the lessons derived from the VA case study. These discussions lasted for a further hour.

The group followed an identifiable process in assessing the acceptability of lessons within their own organisation. They began by assessing whether each issue that arose for the VA was also a significant concern in their hospital. They would then decide whether to accept the recommendation, or customise US recommendations to suit their own context. The acceptance of the lessons were categorised into the following six types reflected in Figure 3,

Implemented. Some of the lessons identified from the VA case study had already been implemented within Chinese security management system. For example, the "Security Policy" recommendation to "Ensure that data security plans for research projects comply with information security policies";

Implemented with customisation. Some of the lessons identified within the VA case study had already been addressed by the organisation but with a slightly different emphasis or approach. For example, for the "Security Policy" recommendation to "Ensure the handling of human subjects in research, complies with HIPAA rules". In the Chinese context, the hospital required that electronic records relating to human subjects were held in compliance with the relevant national data protection laws.

Implementable. Some of the issues identified in the VA incident had not yet been addressed by the Chinese hospital, however, they accepted the need to consider this finding. For example, the VA report recommended changes in the "Management Structure" to "Establish an accurate functional description and performance plan to clarify the line authority and reporting relationship". The Chinese group felt that it would be useful to review their existing practices using the insights

derived from the US case study data breach.

Implementable with customisation. Some of the security issues identified in the VA case study had not been addressed by the organisation, however, the group felt that they could not be implemented without considerable changes within their own organisation. For example, the VA report identified the need to "Re-evaluate and correct position sensitivity levels". This process had not been formalised with the Chinese hospital, hence the focus group rephrased it as "Define position sensitive levels".

Reserved for future use. The penultimate category describes findings that could be reapplied in China but their implementation would take a considerable period of time, for instance where the security management system was not sufficiently mature. For example, the VA recommended that staff "Use encryption, or other effective tools, to protect personal identifiable information stored on removable storage". The Chinese hospital forbade the use of removable media hence this recommendation was not immediately applicable. However, the group could envisage a time when this requirement might be relaxed. If removable media were to be permitted then the VA recommendation would be an essential requirement for future security.

Implementation unnecessary. Some of the US VA recommendations could not be applied in the Chinese healthcare organisation. For example, the previous incident report recommended action to "Develop and issue Government-wide risk analysis criteria". Currently, the redacted hospital interacts with government wide systems, including the Chinese national insurance system. However, they felt that this recommendation could only be implemented at government level, hence it was not a subject they felt was in their area of responsibility.

Figure 3 presents the resulting customised security incident map for the redacted hospital based on the VA case study. As we have seen, the development of a specific security incident map from the GST helps organisations consider their own practices and to assess whether applicable Chinese security standards address the concerns raised in previous breaches from the United States.

6. Discussion

Previous research showed that GSTs can be used to represent and share lessons from previous security incidents [25, 43, 45]. In contrast, this paper has presented empirical studies that evaluate

its acceptance in an industry setting. Through interviews with stakeholders from different roles in a healthcare organisation, we found that the security professionals were very likely to accept GSTs and helped to identify the business scenarios where they might be used. However, healthcare professionals were more reluctant probably because this approach did not fit their existing work patterns or prior knowledge of information security. This can be explained by technological frames [50]. Professionals from different job roles have different interpretations of technology based on their own experience and educational background [50]. Previous research has also identified weaknesses in security incident handling and response [22–24]. Suggestions were made to improve the information sharing, through the integration of agile principles and practices into security incident response [22–25, 43–45, 56]. Our approach evaluated the use of GSTs, in a healthcare context. The results showed that GSTs helped share security lessons with the redacted hospital. The redistribution of security lessons informed their own practices and helped them to assess whether applicable security standards addressed the concerns raised in previous breaches even with those incidents occurred in a different country.

7. Conclusions

The recurrence of past breaches shows that lessons have not been learned from previous security incidents. This paper conducted empirical studies to explore whether or not the recommendations from previous security failures could be redistributed using Generic Security Templates. In particular, we developed a GST from an incident in the United States Veterans Affairs Administration and used it to explore whether lessons could be applied to a healthcare organisation in China. We interviewed ten healthcare professionals and five IT professionals and worked with them to adapt the GST to local standards. The results showed that the security experts in the healthcare organisation accepted this approach and lessons from a US data breach could inform security management in the redacted hospital in China. We have performed the study within one healthcare organisation, therefore, the findings may not reflect potential results from other healthcare organisations around the globe. However, the experience gained from this study provides the basis for future work in conducting similar studies in other countries and with other security cultures.

Acknowledgements

The authors would like to thank the Scottish Informatics and Computer Science Alliance (SICSA) for funding this research.

References

[1] J. J. O'NEILL, Administrative Investigation loss of VA information VA Medical Center Birmingham, AL, Vol. Report No. 07-01083-157, 2007.

[2] C. E. Healthcare, Shenzhen hospital dataloss incident, 2008, http://www.chinaehc.cn/index.php?option=com_content&view=article&id=1937:2010-04-01-09-38-35&catid=15:medical-reforming&Itemid=15 [Online: accessed 18-Nov-2013].

[3] I. C. Office, ICO fines NHS Surrey for failing to check the destruction of old computers, 2013, http://www.ico.org.uk/news/latest_news/2013/ico-issues-nhs-surrey-monetary-penalty-of-200000 [Online: accessed 18-Nov-2013].

[4] Symantec, Internet Security Threat Report 2013, Vol. 18, Symantec Corporation, 2013.

[5] Symantec, Internet Security Threat Report 2014, Vol. 19, Symantec Corporation, 2014.

[6] C. J. Alberts, A. Dorofee, Managing information security risks: the OCTAVE approach, Addison-Wesley Longman Publishing Co., Inc., 2002.

[7] D. W. Bates, R. S. Evans, H. Murff, P. D. Stetson, L. Pizziferri, G. Hripcsak, Detecting adverse events using information technology, Journal of the American Medical Informatics Association 10 (2) (2003) 115–128.

[8] C. Vincent, G. Neale, M. Woloshynowych, Adverse events in British hospitals: preliminary retrospective record review, BMJ 322 (7285) (2001) 517–519.

[9] A. Sheikhtaheri, F. Sadoughi, M. Ahmadi, H. Moghaddasi, A framework of a patient safety information system for Iranian hospitals: lessons learned from Australia, England and the US, International journal of medical informatics 82 (5) (2013) 335–344.

[10] F. Le Duff, S. Daniel, B. Kamendjé, P. Le Beux, R. Duvauferrier, Monitoring incident report in the healthcare process to improve quality in hospitals, International journal of medical informatics 74 (2) (2005) 111–117.

[11] E. Balka, M. Doyle-Waters, D. Lecznarowicz, J. M. FitzGerald, Technology, governance and patient safety: systems issues in technology and patient safety, international journal of medical informatics 76 (2007) S35–S47.

[12] B. Van de Castle, J. Kim, M. L. Pedreira, A. Paiva, W. Goossen, D. W. Bates, Information technology and patient safety in nursing practice: an international perspective, International journal of medical informatics 73 (7) (2004) 607–614.

[13] J. P. Daniels, A. D. King, D. D. Cochrane, R. Carr, N. T. Shaw, J. Lim, J. M. Ansermino, A human factors and survey methodology-based design of a web-based adverse event reporting system for families, International journal of medical informatics 79 (5) (2010) 339–348.

[14] G. Perera, A. Holbrook, L. Thabane, G. Foster, D. J. Willison, Views on health information sharing and privacy from primary care practices using electronic medical records, International journal of medical informatics 80 (2) (2011) 94–101.

[15] S. Haas, S. Wohlgemuth, I. Echizen, N. Sonehara, G. Müller, Aspects of privacy for electronic health records, International journal of medical informatics 80 (2) (2011) e26–e31.

[16] H. van der Linden, D. Kalra, A. Hasman, J. Talmon, Inter-organizational future proof EHR systems: a review of the security and privacy related issues, International journal of medical informatics 78 (3) (2009) 141–160.

[17] GOV.UK, Government launches information sharing partnership on cyber security, 2013, `https://www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security` [Online: accessed 18-Nov-2013].

[18] S. Northcutt, Computer security incident handling: step by step, a survival guide for computer security incident handling, Sans Institute, 2001.

[19] T. Grance, K. Kent, B. Kim, Computer security incident handling guide, NIST Special Publication (2004) 800–61.

[20] N. Direct, National framework for reporting and learning from serious incidents requiring investigation, 2010, `http://www.nrls.npsa.nhs.uk/resources/?entryid45=75173` [Online: accessed 18-Nov-2013].

[21] S. Mitropoulos, D. Patsos, C. Douligeris, On incident handling and response: A state-of-the-art approach, Computers & Security 25 (5) (2006) 351–370.

[22] P. Shedden, A. Ahmad, A. Ruighaver, Organisational learning and incident response: promoting effective learning through the incident response process, School of Computer and Information Science, Edith Cowan University, Perth, Western Australia (2010).

[23] A. Ahmad, J. Hadgkiss, A. B. Ruighaver, Incident response teams–challenges in supporting the organisational security function, Computers & Security 31 (5) (2012) 643–652.

[24] G. Grispos, W. B. Glisson, T. Storer, Rethinking security incident response: The integration of agile principles, arXiv preprint arXiv:1408.2431 (2014).

[25] Y. He, C. Johnson, K. Renaud, Y. Lu, S. Jebriel, An empirical study on the use of the generic security template for structuring the lessons from information security incidents, in: Proceedings of the 6th International Conference on Computer Science and Information Technology, 2014, pp. 178–188.

[26] T. P. Kelly, Arguing safety: a systematic approach to managing safety cases, University of York, 1999.

[27] D. L. Cooke, Learning from incidents, in: 21st System Dynamics Conference, NYC, New York, 2003.

[28] J. Hadgkiss, Computer security incident response teams: Exploring the incident learning capability, Department

of Information Systems, Melbourne, University of Melbourne (2004).

[29] C. P. Waegemann, IT security: developing a response to increasing risks, International journal of bio-medical computing 43 (1) (1996) 5–8.

[30] E. Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general data protection regulation), in: European Network and Information Security Agency, 2012, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf [Online: accessed 16-05-2012].

[31] NH-ISAC, National healthcare and public health resilience, 2013.

[32] A. Greenough, H. Graham, Protecting and using patient information: the role of the caldicott guardian, Clinical medicine 4 (3) (2004) 246–249.

[33] L. Mei, Y. Ling, A study on issues and strategies concerning the IT-based security system for whole people health, China Science & Technology Resources Review 4 (2010) 009.

[34] C.-D. Wang, W.-B. Yang, S.-G. Ju, Research and implementation of electronic health record signature system based on CES, Computer Engineering 16 (2010) 103.

[35] M. Wei, X. Xue-guo, Discussion of patients' confidentiality in sharing electric medical records, Soft Science of Health 3 (2009) 034.

[36] J. Xian-shan, Security control of computer-based patient record, Information of Medical Equipment 2 (2006) 008.

[37] P. SHEN, X.-y. HU, S.-g. ZHANG, D.-j. DU, Informationalized characteristics of medical records management and risk prevention, Journal of Medical Postgraduates 10 (2009) 021.

[38] Y. Cangzhou, L. Zhongkan, Z. Qishan, A security scheme for electronic medical record systems, Computer Engineering 9 (2004) 050.

[39] X. Gao, J. Xu, G. Sorwar, P. Croll, Implementation of e-health record systems and e-medical record systems in china, The International Technology Management Review 3 (2) (2013) 127–139.

[40] B. S. Alhaqbani, Privacy and trust management for electronic health records.

[41] J. Górski, Trust casea case for trustworthiness of IT infrastructures, in: Cyberspace Security and Defense: Research Issues, Springer, 2005, pp. 125–141.

[42] T. Kelly, A systematic approach to safety case management, in: Proc. of SAE 2004 World Congress, Detroit, MI, Citeseer, 2004.

[43] Y. He, C. Johnson, Generic security cases for information system security in healthcare systems, IET, 2012.

[44] Y. He, C. Johnson, M. Evangelopoulou, Z.-S. Lin, Diagraming approach to structure the security lessons: Evaluation using Cognitive Dimensions, in: The 7th International Conference on Trust & Trustworthy Computing, 2014.

[45] Y. He, C. Johnson, Y. Lu, A. Ahmad, Improving the exchange of security arguments in security incident reports: Case studies in the privacy of electronic patient records, in: The 8th IFIP WG 11.11 International Conference on Trust Management, 2014.

[46] R. F. Dacey, Federal Information System Controls Audit Manual (FISCAM), DIANE Publishing, 2010.

[47] GB/T22239-2008 information security technology - base line for classified protection of information system, 2008.

[48] M. of Health of People's republic of China, Guidance on the classified protection of information system by ministry of health, 2011, `http://www.gov.cn/gzdt/2011-12/09/content_2016113.htm` [Online: accessed 18-Nov-2013].

[49] M. B. Miles, A. M. Huberman, Qualitative data analysis: An expanded sourcebook, Sage, 1994.

[50] W. J. Orlikowski, D. C. Gash, Technological frames: making sense of information technology in organizations, ACM Transactions on Information Systems (TOIS) 12 (2) (1994) 174–207.

[51] B. J. Oates, Researching information systems and computing, Sage, 2005.

[52] Y. He, C. Johnson, Improving incident learning in healthcare: An industrial study in the protection of electronic patient records, in: International Journal of Medical Informatics, 2014, under review.

[53] T. Kelly, S. B. Meng, The costs, benefits, and risks associated with pattern based and modular safety case development, in: in Proceedings of the UK MoD Equipment Safety Assurance Symposium, Citeseer, 2005.

[54] T. P. Kelly, Concepts and principles of compositional safety case construction, Contract Research Report for QinetiQ COMSA/2001/1/1 (2001).

[55] E. Madriz, Focus groups in feminist research, Collecting and interpreting qualitative materials 2 (2003) 363–388.

[56] Y. He, C. Johnson, Y. Lu, Y. Lin, Improving the information security management: An industrial study in the privacy of electronic patient records, in: The 27th International Symposium on Computer-Based Medical Systems, 2014.

Appendix A. Participant's background

Table A.3: Participant's background

No.	Position	Education	Incidents Experience	Gender	Years
1	Nurse	Bachelor	Yes	Female	3
2	Nurse	Bachelor	No	Female	2
3	Nurse	Bachelor	Yes	Female	5
4	Nurse	High School	No	Female	3
5	Nurse	High School	No	Female	4
6	Nurse	High School	No	Female	5
7	Doctor	Master	No	Male	8
8	Doctor	Master	Yes	Male	8
9	Doctor	Bachelor (Hon)	No	Male	4
10	Doctor	Bachelor	No	Male	5
11	Security Manager	Bachelor	Yes	Male	8
12	Security Staff	Master	Yes	Female	4
13	Security Staff	Bachelor (Hon)	Yes	Male	2
14	Security Staff	Bachelor (Hon)	Yes	Male	3
15	Security Staff	Bachelor	Yes	Male	2